UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/294,956	04/20/99	COX I	12558

LMC1/0211

PAUL J ESATTO
SCULLY SCOTT MURPHY & PRESSER
400 GARDEN CITY PLAZA
GARDEN CITY NY 11530

EXAMINER	
DI LORENZO,A	
ART UNIT	**PAPER NUMBER**
2766	3

DATE MAILED: 02/11/00

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary	Application No.	Applicant(s)	
	09/294,956	COX ET AL.	
	Examiner	Art Unit	
	Anthony DiLorenzo	2766	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Status

1)☒ Responsive to communication(s) filed on *20 April 1999* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-116* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-116* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claims _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 April 1999* is/are objected to by the Examiner.

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

a)☐ All b)☐ Some * c)☐ None of the CERTIFIED copies of the priority documents have been:

1.☐ received.

2.☐ received in Application No. (Series Code / Serial Number) _____ .

3.☐ received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. & 119(e).

Attachment(s)

14) ☒ Notice of References Cited (PTO-892)
15) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
16) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
17) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
18) ☐ Notice of Informal Patent Application (PTO-152)
19) ☐ Other:

DETAILED ACTION

This Office Action is written in response to papers filed on 20 May 1999 in U.S. Patent Application No. 09/294,956, and to subsequent papers filed pertaining thereto. Claims 1-116 have been examined on the merits.

Drawings

The drawings are objected to by the draftsperson. See enclosed PTO Form 948.

Examiner also objects to the drawings. Figures 1A through 1E should be labeled as "Prior Art" because only that which is old and known in the art is depicted. Applicant is referred to the following references:

1. Kundur and Hatzinakos. "Towards a Telltale Watermarking Technique for Tamper-Proofing." Provided by Applicant in IDS, paper no. 2. See column 2, paragraph 1.

2. US Patent 5,734,752, issued to Knox. See figure 6 and col. 8 lines 31-48.

Specification

The specification is objected to for multiple minor informalities, as listed below. Appropriate correction is required.

1. Page 11, line 13, change "has" to "hash"

2. Page 12, line 30, change "encode" to "leave"

3. Page 15 line 2, delete "be"

4. Page 17 line 26 change "fro" to "from"

Claim Objections

The following text is reproduced from the Manual of Patent Examining Procedure, concerning the treatment of duplicate claims in an application:

> 706.03(k) Duplicate Claims [R - 3]
>
> Inasmuch as a patent is supposed to be limited to only one invention or, at most, several closely related indivisible inventions, limiting an application to a single claim, or a single claim to each of the related inventions might appear to be logical as well as convenient. However, court decisions have confirmed applicant's right to restate (i.e., by plural claiming) the invention in a reasonable number of ways. Indeed, a mere difference in scope between claims has been held to be enough.
>
> Nevertheless, when two claims in an application are duplicates, or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other claim under 37 CFR 1.75 as being a substantial duplicate of the allowed claim.

Claims 92 and 93 are identical and are dependent on the same claim. Accordingly, claim 93 will be objected to under 37 CFR 1.75 as a duplicate of claim 92 if claim 92 is allowed. Examiner suggests canceling claim 93.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 108-111 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 108 recites the limitation "device" in line 2. There is insufficient antecedent basis for this limitation in the claim, since the claim is written to "[a] method for inserting data into digital data." Claims 109-111 contain this fault through nature of their dependence on claim 108. For purposes of applying art, examiner assumed that the claims were written to a method for inserting data into digital data.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 3, 4, 47, 49, 50, 94, and 98 are rejected under 35 U.S.C. 102(b) as being anticipated by Barton ('997).

Claims 1, 3, 47, and 49:
Barton discloses in column 4, lines 15-20, embedding a digital signature of digital data into that data by inserting the signature into predetermined bit positions of the digital data. In column 6, lines 62-65, Barton discloses excluding the predetermined bits from the signature, citing that they will change when the signature is inserted into those bits. The invention of Barton is suitable for signing digital audio, video, and image data (col. 1 line 5).

Claims 4, 50, 94 and 98: Barton is applied as above, and also discloses in column 3, lines 23-30, 45-51 and 58-61, that additional data associated with the digital data, such as a serial number or other identifying information, is also embedded into the digital data and signed. The claim 94 and 98 limitations of receiving data from an external source are also satisfied inherently by Barton. That reference states in column 3, lines 30-47, that embedded authentication data may identify the owner of the digital data. A computer

program/apparatus that performs the method could not by it's nature know the identity of the owner of the digital data. Therefore, that information would have to be supplied by an external source.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2, 5-17, 22-26, 33-37, 42-45, 48, 51-63, 68-72, 79-83, 88-91, 95-97, 99, and 100-107 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barton, as applied above, and further in view of Applied Cryptography, by Bruce Schneier.

Claims 2 and 48: Barton discloses as previously discussed. Barton fails to disclose the use of a hash function signing method. Schneier discloses the well-known method of creating digital signatures using hash functions on page 38, wherein a sender hashes a digital document and encrypts the hash value, thereby creating a signature of the digital document. Since this is a well-known and accepted signing method, it would be within the realm of knowledge of the cryptographer of ordinary skill to implement this method in the invention of Barton. It would be obvious to exclude the predetermined bits from the hash since the hash forms the signature and Barton discloses that the signature should exclude the predetermined bits. Including those bits would significantly change the hash value. If the signature of Barton was then substituted for the predetermined bits (after the hash value had been obtained with the predetermined bits included), that valid signature would always be construed as a forgery because the verification re-hash of the document (created from the copy in which the predetermined bits were overwritten by the signature) would always be different from the original hash value.

The remaining claims rejected under this combination of the prior art are grouped as either "independent" or "dependent" claims.

Independent Claims:

Claims 42 and 88: Barton is applied as for claim 2 above. Schneier also discloses the verification method for said signature as consisting of decrypting the original hash and comparing it to a re-computed hash. If this signing method were used in the invention of Barton, as established above, it would be obvious to the cryptographer of ordinary skill to first extract the signature from the predetermined bits so that verification operations could be performed on it. The obviousness of excluding the predetermined bits from the re-hash is established in the section rejecting claim 2 above.

Claims 104 and 105: Barton is applied as for claim 2 above. Barton does not disclose time stamping of the digital document to be authenticated. Schneier discloses the well-known authentication method of time stamping on pages 38, 59, and 75-76. A particular protocol is described on page 76 ("Improved Arbitrated Protocol") in which time data is appended to a hash value of the document that is to be time stamped. The time data is signed along with the hash value, making the time data authentic. Schneier does not disclose the steps of claim 104 verbatim, but makes them obvious to the cryptographer of ordinary skill. Schneier states on page 59 that timestamps require a secure and accurate system clock. In light of this, the cryptographer of ordinary skill would be motivated to use a tamper resistant chip containing a clock in order to provide accurate time data, in order to obtain the advantages associated with tamper resistant hardware, as would be within the realm of knowledge of the person of ordinary skill. The step of outputting the signature and time data from the clock to the time stamping circuit would be an obvious step to take in any time-stamping method using a secure clock. A circuit would be necessary to concatenate the time and hash data present in the Schneier reference.

Dependent Claims: (all rejections incorporate the rejections of the base claims)
Claims 43, 89, and 106: The invention of Barton is suitable for signing digital audio, video, and image data (col. 1 line 5).

Claims 44 and 90: Barton discloses in col. 3, lines 23-30, 45-51 and 58-61, that additional data associated with the digital data, such as a serial number or other identifying information, is also embedded into the digital data and signed.

Claims 5, 45, 51, and 91: Examiner asserts that in the invention of Barton it would be obvious to insert the additional data into bits of the digital data other than the predetermined bits, since the predetermined bits are already designated for receiving the signature. Any bits residing in the predetermined positions would be overwritten and lost if this were not the case, resulting in an invalid signature.

Claims 6 and 52: Barton discloses in column 7, lines 31-42, that the digital data is divided into blocks (or samples), and that the signature data may be embedded into the least significant bits of a block. Examiner takes official notice that conceptualizing the least significant bits of an image as an LSB plane is old and well known in the art, and may be applied to any image/video/audio data that is divided into blocks (samples).

Claims 7-9 and 53-55: Examiner takes official notice of the following as being old and well-known in the art: a) sampling image data as pixels, b) sampling video data as a particular image position at a particular time (a spatial temporal sample), and c) sampling audio data as a time sample. Since the invention of Barton has been established above to be suited for signing audio/image/video data, and that data is divided into blocks, it would be obvious to use the appropriate sample as the block-type each type of data.

Claims 10 and 56: In the previously cited column 7, lines 31-42, of Barton, all of the embedded data is inserted into the least significant bits, including the signature data and the associated data (see also col. 7, lines 1-5).

Claims 11, 15, 16, 57, 61, and 62: Column 8, lines 31-61, describes transforming a spatially-described image into a frequency-described image, and partitioning the frequency domain into two sections, using Huffman encoding, which takes into account high vs. low frequency components. The predetermined bits are selected from the "least significant bit of a number of the variable length codes in the image."

Claims 12-14 and 58-60: These claims are rejected on the same basis as claims 7-9 and 53-55.

Claims 17 and 63: In column 7, lines 1-5 Barton discloses that additional data indicating the signature calculation technique may be added to the data to be embedded. Since the signing method disclosed in the applied Schneier reference uses a public/private key signing technique, it would be obvious to include identification of the public key in the field mentioned by Barton so that the recipient/verifier could more easily verify the signature.

Claims 18-20 and 64-66: Barton discloses in column 3, lines 31-47, that the associated data may be used to prove ownership of an image by the organization that produced it. From this disclosure, it would be obvious to the person of ordinary skill in data authentication that the associated data may identify any one of a source, owner, or photographer of the digital data.

Claims 21 and 67: Barton discloses adding an error correction code as a field of the associated data after the other parts of the associated data have been encrypted. Therefore the error encryption code of Barton comprises an unencrypted portion of the associated data (col. 7, lines 25-30).

Claims 22-24 and 68-70: Barton discloses in column 7 associated embedded data comprising multiple fields. Claims 23-24 and 69-70 are rejected under the same grounds applied to claims 17 and 63 above, further incorporating the rejection of claims 18-20 above. Given the properties of the combination of prior art (i.e., a public key of the signer and the identity of the owner are included in the associated data, and the signer may also be the owner, it is logical to conclude that the prior art combination would include instances in which the owner of the public key is identified.

Claims 25, 26, 71, 72, 95, 96, 99, and 100: Claim 25 is rejected under the same grounds as claim 4, and further incorporating the rejection of claim 94 above, which specifically addresses data being received from an external source. The examiner takes official notice of the following methods of receiving data as being well-known in the art: Global Positioning Satellite transmissions, radio frequency transmissions received by antennae, and internet transmissions received via a networked computer. These methods of importing external data are all within the realm of knowledge of the person of ordinary skill and would be obvious to include in the invention of Barton since external data must be imported.

Claims 33 and 79: The rejection of claims 6 and 52 above is incorporated. Barton does not disclose inserting the additional data before signing. In the Barton reference, the additional data is concatenated to the signature, then both are embedded. However, examiner takes official notice that it would be within the realm of knowledge of the person of ordinary skill in cryptography to include the additional data with the original digital data before signing, so that the signature would encompass both entities. This would increase the security of the additional data. In column 3, line 48, through column 4, line 8, Barton provides motivation for including this feature in the invention of that reference. Barton states that the embedded meta-data (additional data) should be secured by a digital signature.

Claims 34-37 and 80-83: The rejection of independent claims 104 and 105 is incorporated. The well known method of time stamping disclosed in the cited Schneier reference discloses that the actual operations are performed by a trusted third party in order to time stamp a document. Encrypting a hash of the time stamp and first hash would be within the knowledge of the person of ordinary skill in cryptography as a way of shortening the amount of data that needs to be processed, transmitted, and/or encrypted, and would be an obvious step in reducing overhead in those areas. It would also be obvious to the cryptographer of ordinary skill dealing in network security to use and Internet service provider to perform the time stamping operations, in order to make it unnecessary for each user of a time stamping service to obtain a tamper resistant chip, thereby making a time stamping product more affordable to the consumer.

Claims 97 and 101: Claims 97 and 101 are rejected under the same grounds as claim 2 above, those grounds further comprising that a signature authenticating that a document has not been tampered with comprises authentication of information associated with the digital data.

Claims 102, 103, and 107: Because the invention of Barton is specifically intended to process digital image, video and audio data, it would be obvious to use a digital image generation device to generate a digital image. Examiner takes official notice that scanners, digital cameras, and digital video cameras are well known in the art of digital image generation and it would be well within the knowledge of the person of ordinary skill to use these devices.

Claims 27-32, 46, 73-78, 92, and 93 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barton in view Schneier, as applied above, and further in view of Conner et al. ('393).

Claims 27, 30, 73, and 76: The cryptographer of ordinary skill is assumed to have within his/her realm of knowledge that most types of compression result in lost data (general computer knowledge), and that a digital signature of the type disclosed in Schneier and applied above will be considered a forgery if an attempt is made to verify data from which any bits have been lost, as is the case when a data undergoes lossy compression. For example, if a bitmap image is signed and then compressed under JPEG compression, the resulting JPEG image, even if decompressed, will not contain the same data as the

original bitmap image. Therefore, when the JPEG image (compressed or decompressed) is hashed, that hash value would not agree with the decrypted signature that was generated from the original bitmap. Given this knowledge, it would be obvious to the cryptographer of ordinary skill to sign the set of data that is to be verified, and not prior forms of the data. The claims further specify that the signature is inserted into the header of the compressed digital data. Conner et al. disclose the feature of inserting a digital signature into a header of the data that it authenticates (fig. 8A element 104 and col. 9, lines 3-15). It would be obvious to the cryptographer of ordinary skill to use this feature in the combination of Barton and Schneier if that data were to be compressed, because the signature could not be inserted into the compressed data for lack of available bits after the compression: it is well-known to attach a signature to its associated data, and headers are well-known places for inserting information about data.

Claims 28, 29, 31, 32, 74, 75, 77, and 78: Barton discloses the use of JPEG and MPEG compression in column 8 line 30 through column 9 line 45.

Claims 46, 92, and 93: The information presented in the rejection of claims 27, 30, 73, and 76, above, is incorporated. Decompressing a compressed file is well known in the art and would be an obvious operation to perform on any previously compressed file. The claimed limitation of moving the signature from the header to the predetermined bits would also be an obvious step to the person of ordinary skill. Motivation to include this step in the combination of references stems from the mathematical concept of solving a problem by transforming it into a problem that has already been solved. The invention of Barton already has written into it a way of extracting the signature from the predetermined bits for authentication. The person of ordinary skill would be motivated to find a way to use this signature extraction process for compressed data as well, rather than create a new signature verification process altogether. Moving the signature data to the predetermined bits simply reduces the signature extraction problem to one that has already been solved in Barton.

Claims 38-41, 84-87, and 108-116 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barton in view of Schneier, as applied above, and further in view of Bramall ('101).

Claims 38, 84, 108-110, 112, and 115: Barton and Schneier fail to disclose recognizing an authorized user of digital equipment and inserting an identifier thereof into the digital data. Bramall discloses a security system for data handling equipment wherein a pre-authorized user of digital image data generating equipment is recognized by the equipment. The data processed by that user is merged with an identifier of the user and recorded on a digital storage means. See Bramall column 2, line 58 through column 3, line 20. Upon gaining knowledge of this reference, the person of ordinary skill in cryptography would be motivated to include the user recognition/recording properties of Bramall in the invention of Barton. Motivation for this inclusion exists in both Bramall and Barton. One of the purposes of Bramall's invention is to identify the user who processed a particular digital record. Barton states on column 3 that a function of embedded authentication data is to detect illegal copying. A digital data generation

device that records each user's identity could be an effective deterrent against the production of illegal copies of digital property.

Claims 39, 85, 113: (private key stored with identifier) The primary reference (Barton) discloses signing of the digital data. Examiner takes official notice that the use of a public/private key pair for signing digital data is a well known method and the person of ordinary skill would be motivated to use it in Barton so that anyone with the public key would be able to verify the signature. Since the intent of Barton's invention is to sign the data to prove ownership, and the obviousness of recognizing and identifying the owner of the data has been established as per Bramall, the person of ordinary skill would be motivated associate a key with a corresponding identity in memory in order to prevent malicious users from making false associations manually.

Claims 40, 86, 114: Examiner takes official notice that fingerprint recognition is a well known form of identification that falls under the general topic of biometrics, and would be obvious to use to identify the user of Bramall to gain the advantages associated with biometrics. Exemplary advantages are that biometrics are not easily forgeable and cannot be lost by users.

Claims 41, 87, 111: Examiner takes official notice that a name is a well-known form of identifier and would be obvious to use as the identification in the invention of Bramall. Motivation includes the fact that records of the data are stored on a CD-ROM and may be subject to review by a human operator, whom would most likely find it more comfortable to search through names rather than other forms of identification, such as an arbitrary number.

Claim 116: Rejected on the same grounds as claim 107, in addition to the grounds of rejection for claim 112.

Conclusion

The following prior art made of record but not previously cited is considered pertinent to the applicant's disclosure:

1. US Patent 5,898,779 issued to Squilla et al. discloses a digital camera having an embedded unique private key for digitally signing images taken by the camera, and specifically discloses in column 8, lines 20-33 that if an image is signed and then undergoes lossy compression, that signature will be flagged as invalid.

2. US Patent 5,870,499 issued to Bender et al. discloses a method for embedding recoverable data such as a digital signature in digital images by altering randomly selected luminance values.

3. US Patent 5,742,771 issued to Fontaine discloses embedding of digital signatures into the least significant bits of audio data.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Anthony DiLorenzo, whose telephone number is (703) 306-5617. The examiner can normally be reached on Monday-Thursday from 8:00 a.m. to 5:30 p.m. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes, can be reached at (703) 305-9711. The official fax phone number for the organization where this application or proceeding is assigned is (703) 308-~~9051~~ 0540. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Anthony DiLorenzo

AD

2/8/00

2/8/2000

GILBERTO BARRON, JR.
PRIMARY EXAMINER
ART UNIT ~~222~~ 2767